

Beschreibung

Einräumung eines Zugriffs auf ein computerbasiertes Objekt

- 5 Die vorliegende Erfindung betrifft ein Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt und ein Steuerungsprogramm zur Durchführung des Verfahrens.

- 10 Durch unberechtigte Benutzung von Computerprogrammen entstehen weltweit immense Schäden. Um diesem entgegenzuwirken, werden Lösungen zum Schutz von Computerprogrammen vor unberechtigter Benutzung entwickelt.

- 15 Eine Übermittlung verschlüsselter Informationen zur Aktivierung eines Computerprogramms dient einer Verhinderung von nicht autorisierten Vervielfältigungen des Computerprogramms. Entsprechende Verfahren dienen beispielsweise außerdem als technische Voraussetzung, um Computerprogramme als Produkte über E-Commerce zu vertreiben. Bei bisher bekannten Verfahren
- 20 zur Aktivierung von Computerprogrammen werden Computerprogramme anhand jeweils eines Registrierungsschlüssels freigeschaltet. Für eine Freischaltung eines Computerprogramms wird der Registrierungsschlüssel, der einer Computerprogrammlicenz fest zugeordnet ist, manuell eingegeben bzw. von einem Datenträger eingespielt. Insbesondere bei einer Vielzahl von auf
- 25 unterschiedlichen Computern installierten Computerprogrammen resultiert hieraus ein hoher Administrationsaufwand, der mit personalintensiven Bedien- und Wartungsarbeiten verbunden ist.

- 30 Aus EP 1 191 419 A2 ist Verfahren bekannt, bei dem vorgebbare Funktionen eines Computerprogramms für eine wählbare Nutzungsdauer durch Modifikation eines Registrierungsschlüsselpaares freigeschaltet werden können. Das Registrierungsschlüsselpaars weist zumindest eine gegenüber Benutzer-
- 35 zugriffen gesperrten Teilinformation auf. Die freizuschaltenden Funktionen müssen nicht notwendigerweise bereits bei ei-

ner Erstinstallation des Computerprogramms für eine Freischaltung zur Verfügung gestanden haben, sondern können auch nachträglich hinzugewählt werden. Zur Freischaltung ist kein Einsatz von Bedien- und Wartungspersonal am Ort des Computers erforderlich, auf der das jeweilige Computerprogramm installiert ist.

Bestandteile des Registrierungsschlüsselpaares entsprechend dem in EP 1 191 419 A2 beschriebenen Verfahren sind Applikationsinformationen und ein Applikationswert. Die Applikationsinformationen werden an einem ersten Computer eingegeben, auf der das zu registrierende Computerprogramm installiert ist, bzw. durch den ersten Computer generiert. Der Applikationswert wird in einem zweiten Computer mittels Codierung aus den Applikationsinformationen berechnet.

Bei einer Registrierung eines Computerprogramms oder einer Änderung der Registrierung werden erste Applikationsinformationen mit zumindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation an den zweiten Computer übermittelt. Im zweiten Computer wird aus den ersten Applikationsinformationen ein Applikationswert berechnet, der nachfolgend an den ersten Computer übermittelt wird. Mittels Decodierung werden im ersten Computer aus dem Applikationswert zweite Applikationsinformationen ermittelt. Die ersten und die zweiten Applikationsinformationen werden bei einem Ausführungsbeginn des Computerprogramms auf Übereinstimmung überprüft. In Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen werden vorgebbare Funktionen des Computerprogramms freigeschaltet.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde ein Verfahren, das einen erhöhten Schutz vor unberechtigter Benutzung von in einer Recheneinrichtung bereitgestellten Ressourcen bietet, sowie eine zur automatisierten Durchführung des Verfahrens geeignete Implementierung anzugeben.

3

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 und ein Steuerungsprogramm mit den in Anspruch 10 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Erfindungsgemäß resultiert ein erhöhter Schutz vor unberechtigter Benutzung von in einer Recheneinrichtung bereitgestellten Ressourcen daraus, daß als eine Voraussetzung zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt eine Speicherkarte mit einem Programmcodeprozessor und eine Lizenzinformation bereitgestellt werden. Auf der Speicherkarte sind zumindest ein der Speicherkarte zugeordneter öffentlicher und privater Schlüssel abgespeichert. Die Lizenzinformation umfaßt zumindest einen mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode und wird an einer den Zugriff auf das computerbasierte Objekt steuernden Recheneinrichtung bereitgestellt.

Erfindungsgemäß wird aus einer von der Speicherkarte generierten ersten Zufallszahl und aus einer durch die Recheneinrichtung bereitgestellten zweiten Zufallszahl ein symmetrischer Schlüssel erzeugt, der für die Speicherkarte und die Recheneinrichtung zugänglich gemacht wird. Der verschlüsselte Lizenzcode und eine mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehene Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes werden an die Speicherkarte übermittelt. Der verschlüsselte Hash-Wert wird von der Speicherkarte entschlüsselt und mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert auf Übereinstimmung überprüft. Bei positivem Überprüfungsergebnis wird die Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte ausgeführt und ein entschlüsselter Lizenzcode an die Recheneinrichtung übermittelt. Der entschlüsselte Lizenzcode wird dann zumindest temporär zum Zugriff auf das computerbasierte Objekt bereitgestellt.

- Unter Recheneinrichtung sind beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs PCs, Notebooks, Server, PDAs, Mobiltelefone, Geldautomaten, Steuerungsmodule in der
- 5 Automatisierungs-, Fahrzeug-, Kommunikations- oder Medizintechnik zu verstehen - allgemein Einrichtungen, in denen Computerprogramme ablaufen können. Des weiteren sind computerbasierte Objekte beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs Betriebssysteme, Steuerungs- oder
- 10 Anwendungsprogramme, durch Betriebssysteme, Steuerungs- oder Anwendungsprogramme bereitgestellte Dienste, Leistungsmerkmale, Funktionen oder Prozeduren, Zugriffsrechte auf Peripheriegeräte sowie auf einem Speichermedium befindliche Daten.
- 15 Entsprechend einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird der öffentliche Schlüssel der vertrauenswürdigen Instanz vor Manipulationen geschützt an der Recheneinrichtung bereitgestellt. Außerdem ist die Lizenzinformation mittels eines privaten Schlüssels der vertrauenswürdigen
- 20 Instanz digital signiert. Die digitale Signatur der Lizenzinformation kann somit in der Recheneinrichtung anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft werden. Auf diese Weise kann eine vertrauenswürdige und sichere Übermittlung der Lizenzinformation zur Recheneinrichtung
- 25 gewährleistet werden.
- Der entschlüsselte Lizenzcode kann mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehen werden. Der verschlüsselte Hash-Wert des entschlüsselten
- 30 Lizenzcodes kann dann in der Recheneinrichtung entschlüsselt und mit einem für den entschlüsselten Lizenzcode berechneten Hash-Wert auf Übereinstimmung überprüft werden. Dies bietet den Vorteil, daß sichergestellt ist, daß der Lizenzcode tatsächlich mit der zur Entschlüsselung vorgesehenen Speicherkarte entschlüsselt worden ist.
- 35

Vorzugsweise ist der symmetrische Schlüssel nur für einen Zugriffseinräumungsvorgang gültig und wird bei jeder Zugriffsanforderung neu erzeugt. Dies trägt zu einer weiteren Erhöhung der Sicherheit gegenüber Manipulationsversuchen bei.

5

Vorteilhafterweise umfaßt die Lizenzinformation zusätzlich den der Speicherkarte zugeordneten öffentlichen Schlüssel. Des weiteren wird die erste Zufallszahl mittels des der Speicherkarte zugeordneten privaten Schlüssels digital signiert an die Recheneinrichtung übermittelt wird. Die digitale Signatur der ersten Zufallszahl wird dann in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels überprüft. Die zweite Zufallszahl wird mittels des öffentlichen Schlüssels der Speicherkarte verschlüsselt an die Speicherkarte übermittelt und dort entschlüsselt. Diese Weiterbildung bietet den Vorteil einer gesicherten Übertragung der ersten und zweiten Zufallszahl zur Erzeugung des symmetrischen Schlüssels.

20 Entsprechend einer weiteren vorteilhaften Ausgestaltung der vorliegenden Erfindung werden der verschlüsselte Lizenzcode und die mit dem verschlüsselten Hash-Wert versehene Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt. Hierdurch werden Manipulationsmöglichkeiten zur unberechtigten Erlangung des Zugriffs auf das computerbasierte Objekt weiter eingeschränkt.

30 Vorteilhafterweise wird durch die Speicherkarte eine dritte Zufallszahl erzeugt und diese an die Recheneinrichtung übermittelt. Durch die Recheneinrichtung kann dann für die Angabe der von der Speicherkarte auszuführenden Funktion ein Hash-Wert, der mittels des symmetrischen Schlüssels und der dritten Zufallszahl verschlüsselt wird, berechnet und verschlüsselt an die Speicherkarte übermittelt werden. Der mittels des symmetrischen Schlüssels und der dritten Zufallszahl ver-

schlüsselte Hash-Wert wird schließlich durch die Speicherkarte entschlüsselt und mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert auf Übereinstimmung überprüft. Hierdurch ergibt sich ein

5 wirksamer Wiederholungsschutz, so daß ein Abfangen von zwischen der Speicherkarte und der Recheneinrichtung ausgetauschten Signalen keine wirksamen Manipulationsmöglichkeiten eröffnet. Außerdem bietet diese Ausgestaltung den Vorteil, daß verfügbare Secure-Messaging-Verfahren für eine Übermittlung eines entsprechenden Funktionsaufrufs zur Ent-

10 schlüsselung des Lizenzcodes verwendet werden können.

Zur Gewährleistung eines Wiederholungsschutzes in bezug auf eine Übermittlung des entschlüsselten Lizenzcodes an die Recheneinrichtung wird entsprechend einer weiteren Ausgestaltung in der Recheneinrichtung eine vierte Zufallszahl erzeugt und diese an die Speicherkarte übermittelt. Durch die Speicherkarte wird dann für den entschlüsselten Lizenzcode ein Hash-Wert, der mittels des symmetrischen Schlüssels und der

15 vierten Zufallszahl verschlüsselt wird, berechnet und verschlüsselt an die Recheneinrichtung übermittelt. Der mittels des symmetrischen Schlüssels und der vierten Zufallszahl verschlüsselte Hash-Wert kann anschließend in der Recheneinrichtung entschlüsselt und mit einem für den entschlüsselten Lizenzcode berechneten Hash-Wert auf Übereinstimmung überprüft werden.

20

25

Entsprechend einer bevorzugten Ausgestaltung der vorliegenden Erfindung werden zur Einräumung des Zugriffs auf das computerbasierte Objekt der entschlüsselte Lizenzcode und ein Überprüfungsprozeßverlauf mit einer jeweiligen Soll-Vorgabe abgeglichen. Dies bietet zusätzliche Sicherheit, da ein Vorliegen des entschlüsselten Lizenzcodes für eine Zugriffsberechtigung alleine nicht mehr ausreichend ist, sondern an einen erfolgreichen Überprüfungsprozeßverlauf gekoppelt ist.

30

35

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert.

5 Es zeigt die Figur eine schematische Darstellung eines Anwendungsumfeldes der vorliegenden Erfindung mit einem Informations- und Meldungs-
austausch zwischen einer vertrauenswürdigen Instanz, einer den Zugriff auf ein computerbasiertes Objekt steuernden Recheneinrichtung und einer Speicherkarte mit Programmcodeprozessor.

10

Das in der Figur dargestellte Anwendungsumfeld der vorliegenden Erfindung umfaßt eine vertrauenswürdige Instanz 10, einen Computer 20, ein mit dem Computer 20 verbundenes Smartcard-Terminal 30, in das eine Smartcard 40 einführbar ist. Die
15 vertrauenswürdige Instanz 10 kann beispielsweise einem Hersteller einer gegen unberechtigten Zugriff zu schützenden Software zugeordnet sein und übernimmt eine Verwaltung von Lizenzen und zu Smartcards zugeordnetem Schlüsselmaterial. Der vertrauenswürdigen Instanz 10 ist ferner ein asymmetrisches
20 Schlüsselpaar 11 zugeordnet, das einen privaten und einen öffentlichen Schlüssel umfaßt. Zur Abspeicherung des zu Smartcards zugeordnetem Schlüsselmaterial ist eine Datenbasis 12 vorgesehen, welche öffentliche Schlüssel auszuliefernder bzw. bereits ausgelieferter Smartcards enthält.

25

Durch den Computer 20 werden für einen oder mehrere Benutzer Systemressourcen 22 verfügbar gemacht, die beispielsweise Programme oder Speicherbereiche mit Daten umfassen. Das hier beschriebene Verfahren zur Einräumung eines Zugriffs auf ein
30 computerbasiertes Objekt ist grundsätzlich auf beliebige Systemressourcen anwendbar. Der Computer 20 steuert insbesondere einen Zugriff auf die Systemressourcen 22, die im vorliegenden Fall auch Software des Herstellers umfassen, welchem die vertrauenswürdige Instanz 10 zugeordnet ist. Des weiteren
35 wird der öffentliche Schlüssel 21 der vertrauenswürdigen Instanz 10 vor Manipulation geschützt am Computer 20 bereitgestellt.

Mit dem Computer 20 ist das Smartcard-Terminal 30 über eine gesicherte Kommunikationsverbindung verbunden. Das Smartcard-Terminal 30 dient zum Informations- und Meldungsaustausch zwischen dem Computer 20 und einer in das Smartcard-Terminal 30 einführbaren Smartcard 40, die eine Speicherkarte mit einem Programmcodeprozessor darstellt. Auf der Smartcard 40 ist ein der Smartcard 40 zugeordnetes asymmetrisches Schlüssel-paar 41 abgespeichert, das einen öffentlichen und einen privaten Schlüssel der Smartcard 40 umfaßt. Außerdem ist auf der Smartcard 40 zumindest ein Programm vorgesehen zur Ver- und Entschlüsselung unter Nutzung des asymmetrischen Schlüssel-paares 42 der Smartcard 40. Darüber hinaus verfügt die Smartcard 40 über einen Zufallszahlengenerator und ist vorzugsweise konform zu ISO 7816/8.

Am Computer 20 wird eine von der vertrauenswürdigen Instanz 10 erstellte Lizenzinformation 1 bereitgestellt. Die Lizenzinformation 1 umfaßt einen mittels des der Smartcard 40 zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode (`enc_SC(licencecode)`) und den der Smartcard 40 zugeordneten öffentlichen Schlüssel (`pub_SC`). Des weiteren ist die Lizenzinformation 1 mittels des privaten Schlüssels der vertrauenswürdigen Instanz 10 digital signiert (`sig_TP`), so daß die digitale Signatur der Lizenzinformation 1 im Computer 20 anhand des öffentlichen Schlüssels 21 der vertrauenswürdigen Instanz 10 überprüft werden kann.

Zur Erzeugung eines symmetrischen Schlüssels (K) 24, 43, der nur für einen Zugriffseinräumungsvorgang gültig ist und bei jeder Zugriffsanforderung neu zu erzeugen ist, wird zunächst die Smartcard 40 mittels einer Anforderungsmeldung 2a (Get-Challenge) des Computers 20 zur Erzeugung einer ersten Zufallszahl (`rand1`) aufgefordert. Nach Erzeugung der ersten Zufallszahl durch die Smartcard 40 wird die Anforderungsmeldung 2a durch Übermittlung einer Ergebnismeldung 2b (`rand1`) mit der ersten Zufallszahl beantwortet. Je nach Sicherheitsanfor-

derung kann die erste Zufallszahl auch mit dem privaten Schlüssel der Smartcard 40 digital signiert an den Computer 20 übermittelt und dort verifiziert werden werden.

- 5 Nach Empfang der ersten Zufallszahl erzeugt der Computer 20 eine zweite Zufallszahl (rand2) und übermittelt diese unter Anwendung von Secure-Messaging durch ein mit dem öffentlichen Schlüssel der Smartcard 40 verschlüsseltes Mutual-Authenticate-Kommando 3a (SM_enc_SC(MutAuth())) an die Smartcard 40.
- 10 Das Mutual-Authenticate-Kommando 3a umfaßt die zweite Zufallszahl sowie einen zur ersten Zufallszahl unter Verwendung eines weiteren symmetrischen Schlüssels (S) 23, 42 gebildeten Message-Authentication-Code (MAC_S). Der weitere symmetrische Schlüssel 23, 42 ist sowohl im Computer 20 als auch auf
- 15 der Smartcard 40 gespeichert, dient einer gegenseitigen Authentifizierung zwischen dem Computer 20 und der Smartcard 40 und braucht nicht notwendigerweise geheim gehalten zu werden. Der zur ersten Zufallszahl gebildete Message-Authentication-Code umfaßt neben der ersten Zufallszahl einen für die
- 20 erste Zufallszahl gebildeten und mit dem weiteren symmetrischen Schlüssel 23, 42 verschlüsselten Hash-Wert.

- Zur Bestätigung einer erfolgreichen Entschlüsselung des Mutual-Authenticate-Kommandos sowie Überprüfung des Message-
- 25 Authentication-Codes und damit des Empfangs der zweiten Zufallszahl wird eine Bestätigungsmeldung 3b an den Computer 20 übermittelt. Somit ist sichergestellt, daß die erste und zweite Zufallszahl sowohl im Computer 20 als auch auf der Smartcard 40 zur Erzeugung des symmetrischen Schlüssels 24,
- 30 43 vorliegen. Die Erzeugung des symmetrischen Schlüssels erfolgt dann im Computer 20 und auf der Smartcard 40 unabhängig voneinander. Der symmetrische Schlüssel 24, 43 ist somit sowohl im Computer 20 als auch auf der Smartcard 40 zumindest für die Dauer eines Zugriffseinräumungsvorgangs verfügbar.
- 35 Durch die Erzeugung des symmetrischen Schlüssels 24, 43 ist eine Grundlage dafür gelegt, später einen Funktionsaufruf zur Entschlüsselung des Lizenzcodes (PSO_DEC - perform securitiy

10

operation mode decrypt, angewendet auf den mittels des öffentlichen Schlüssels der Smartcard 40 verschlüsselten Lizenzcode) unter Anwendung von Secure-Messaging an die Smartcard 40 zu übermitteln.

5

Nachfolgend wird die Smartcard 40 zur Realisierung eines Wiederholungsschutzes mittels einer Anforderungsmeldung 4a (Get-Challenge) des Computers 20 zur Erzeugung einer dritten Zufallszahl (rand3) aufgefordert. Nach Erzeugung der dritten Zufallszahl durch die Smartcard 40 wird die Anforderungsmeldung 4a durch Übermittlung einer Ergebnismeldung 4b (rand3) mit der dritten Zufallszahl beantwortet. Anschließend wird im Computer 20 eine vierte Zufallszahl (rand4) erzeugt und diese mittels einer Meldung 5a (GiveRandom) an die Smartcard 40 übermittelt. Von der Smartcard 40 wird der Empfang der vierten Zufallszahl durch eine Bestätigungsmeldung 5b quittiert.

Nach quittierter Übermittlung der vierten Zufallszahl wird eine Meldung 6a zur Entschlüsselung des Lizenzcodes vom Computer 20 an die Smartcard 40 übermittelt. Die Meldung 6a zur Entschlüsselung des Lizenzcodes umfaßt neben dem verschlüsselten Lizenzcode eine Angabe einer von der Smartcard 40 auszuführenden Funktion zur Entschlüsselung des Lizenzcodes. Die Angabe der von der Smartcard 40 auszuführenden Funktion ist mit einem Hash-Wert versehen, der mittels des symmetrischen Schlüssels 24, 43 und der dritten Zufallszahl verschlüsselt ist. Der mittels des symmetrischen Schlüssels 24, 43 und der dritten Zufallszahl verschlüsselte Hash-Wert wird anschließend durch die Smartcard 40 entschlüsselt und mit einem für die Angabe der von der Smartcard 40 auszuführenden Funktion berechneten Hash-Wert auf Übereinstimmung überprüft.

Bei einem positivem Überprüfungsergebnis wird die Funktion zur Entschlüsselung des Lizenzcodes durch die Smartcard 40 ausgeführt und ein entschlüsselter Lizenzcode mittels einer Meldung 6b unter Anwendung von Secure-Messaging an den Computer 20 übermittelt. Zur Anwendung von Secure-Messaging be-

11

rechnet die Smartcard 40 für den entschlüsselten Lizenzcode einen Hash-Wert, der mittels des symmetrischen Schlüssels 24, 43 und der vierten Zufallszahl verschlüsselt wird. Dieser verschlüsselte Hash-Wert wird zusammen mit dem entschlüsselten Lizenzcode an den Computer 20 übermittelt. Dort wird der Hash-Wert anschließend mittels des symmetrischen Schlüssels 24, 43 und der vierten Zufallszahl entschlüsselt und mit einem für den entschlüsselten Lizenzcode berechneten Hash-Wert auf Übereinstimmung überprüft.

10

Bei Übereinstimmung der Hash-Werte wird der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf die geschützte Software bzw. ein computerbasiertes Objekt bereitgestellt. Um denkbare Manipulationsmöglichkeiten auszuschließen, sollten der entschlüsselte Lizenzcode und ein Überprüfungsprozeßverlauf mit einer jeweiligen Soll-Vorgabe vor Einräumung des Zugriffs auf die geschützte Software abgeglichen werden. Bei erfolgreichem Abgleich kann dann der Zugriff eingeräumt werden.

20

Die Steuerung des Ablaufs des Verfahrens zur Einräumung eines Zugriffs auf geschützte Software bzw. ein computerbasiertes Objekt ist durch ein Steuerungsprogramm implementiert, das in einem Arbeitsspeicher des Computers 20 ladbar ist und zumindest ein Codeabschnitt aufweist, bei dessen Ausführung zunächst eine Erzeugung eines symmetrischen Schlüssels aus einer von einer Speicherkarte mit einem Programmcodeprozessor generierten ersten Zufallszahl und aus einer durch die Recheneinrichtung bereitgestellten zweiten Zufallszahl veranlaßt wird. Ferner wird eine Übermittlung eines mittels der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcodes und einer mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehenen Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes an die Speicherkarte veranlaßt. Des weiteren wird bei Ausführung eine Entschlüsselung des verschlüsselten Hash-Werts durch die Speicherkarte

35

und eine Überprüfung auf Übereinstimmung mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert veranlaßt. Bei positivem Überprüfungsergebnis werden dann eine Ausführung der Funktion zur Ent-

5 schlüsselung des Lizenzcodes durch die Speicherkarte und eine Übermittlung eines verschlüsselten Lizenzcodes an den Computer 20 veranlaßt. Schließlich wird bei Ausführung des Codeabschnittes der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt durch den Computer

10 20 bereitgestellt, wenn das Steuerungsprogramm im Computer 20 abläuft.

Die Anwendung der vorliegenden Erfindung ist nicht auf das hier beschriebene Ausführungsbeispiel beschränkt.

Patentansprüche

1. Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt, bei dem

- 5 - eine Speicherkarte mit einem Programmcodeprozessor bereitgestellt wird, auf der zumindest ein der Speicherkarte zugeordneter öffentlicher und privater Schlüssel abgespeichert sind,
- 10 - eine Lizenzinformation, die zumindest einen mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode umfaßt, an einer den Zugriff auf das computerbasierte Objekt steuernden Recheneinrichtung bereitgestellt wird,
- 15 - aus einer von der Speicherkarte generierten ersten Zufallszahl und aus einer durch die Recheneinrichtung bereitgestellten zweiten Zufallszahl ein symmetrischer Schlüssel erzeugt wird, der für die Speicherkarte und die Recheneinrichtung zugänglich gemacht wird,
- 20 - der verschlüsselte Lizenzcode und eine mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehene Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes an die Speicherkarte übermittelt werden,
- 25 - der verschlüsselte Hash-Wert von der Speicherkarte entschlüsselt und mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert auf Übereinstimmung überprüft wird,
- 30 - bei positivem Überprüfungsergebnis die Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte ausgeführt und ein entschlüsselter Lizenzcode an die Recheneinrichtung übermittelt wird,
- der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt bereitgestellt wird.

35

2. Verfahren nach Anspruch 1,

- bei dem der öffentliche Schlüssel der vertrauenswürdigen Instanz vor Manipulationen geschützt an der Recheneinrichtung bereitgestellt wird, bei dem die Lizenzinformation mittels eines privaten Schlüssels der vertrauenswürdigen Instanz digital signiert ist, und bei dem die digitale Signatur der Lizenzinformation in der Recheneinrichtung anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft wird.
- 5
- 10 3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem der entschlüsselte Lizenzcode mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehen wird, und bei dem der verschlüsselte Hash-Wert des entschlüsselten Lizenzcodes in der Recheneinrichtung entschlüsselt und mit einem für den entschlüsselten Lizenzcode berechneten Hash-Wert auf Übereinstimmung überprüft wird.
- 15
4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem der symmetrische Schlüssel nur für einen Zugriffseinträglichungsvorgang gültig ist und bei jeder Zugriffsanforderung neu erzeugt wird.
- 20
5. Verfahren nach einer der Ansprüche 1 bis 4, bei dem
- 25 - die Lizenzinformation zusätzlich den der Speicherkarte zugeordneten öffentlichen Schlüssel umfaßt,
- die erste Zufallszahl mittels des der Speicherkarte zugeordneten privaten Schlüssels digital signiert an die Recheneinrichtung übermittelt wird,
- 30 - die digitale Signatur der ersten Zufallszahl in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels überprüft wird,
- die zweite Zufallszahl mittels des öffentlichen Schlüssels der Speicherkarte verschlüsselt an die Speicherkarte übermittelt und dort entschlüsselt wird.
- 35
6. Verfahren nach einem der Ansprüche 1 bis 5,

der verschlüsselte Lizenzcode und die mit dem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehene Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von
5 der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt werden.

7. Verfahren nach einem der Ansprüche 1 bis 6,
bei dem durch die Speicherkarte eine dritte Zufallszahl erzeugt und diese an die Recheneinrichtung übermittelt wird,
10 bei dem durch die Recheneinrichtung für die Angabe der von der Speicherkarte auszuführenden Funktion ein Hash-Wert, der mittels des symmetrischen Schlüssels und der dritten Zufallszahl verschlüsselt wird, berechnet und verschlüsselt an die
15 Speicherkarte übermittelt wird, und bei dem der mittels des symmetrischen Schlüssels und der dritten Zufallszahl verschlüsselte Hash-Wert durch die Speicherkarte entschlüsselt und mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert auf Übereinstimmung
20 überprüft wird.

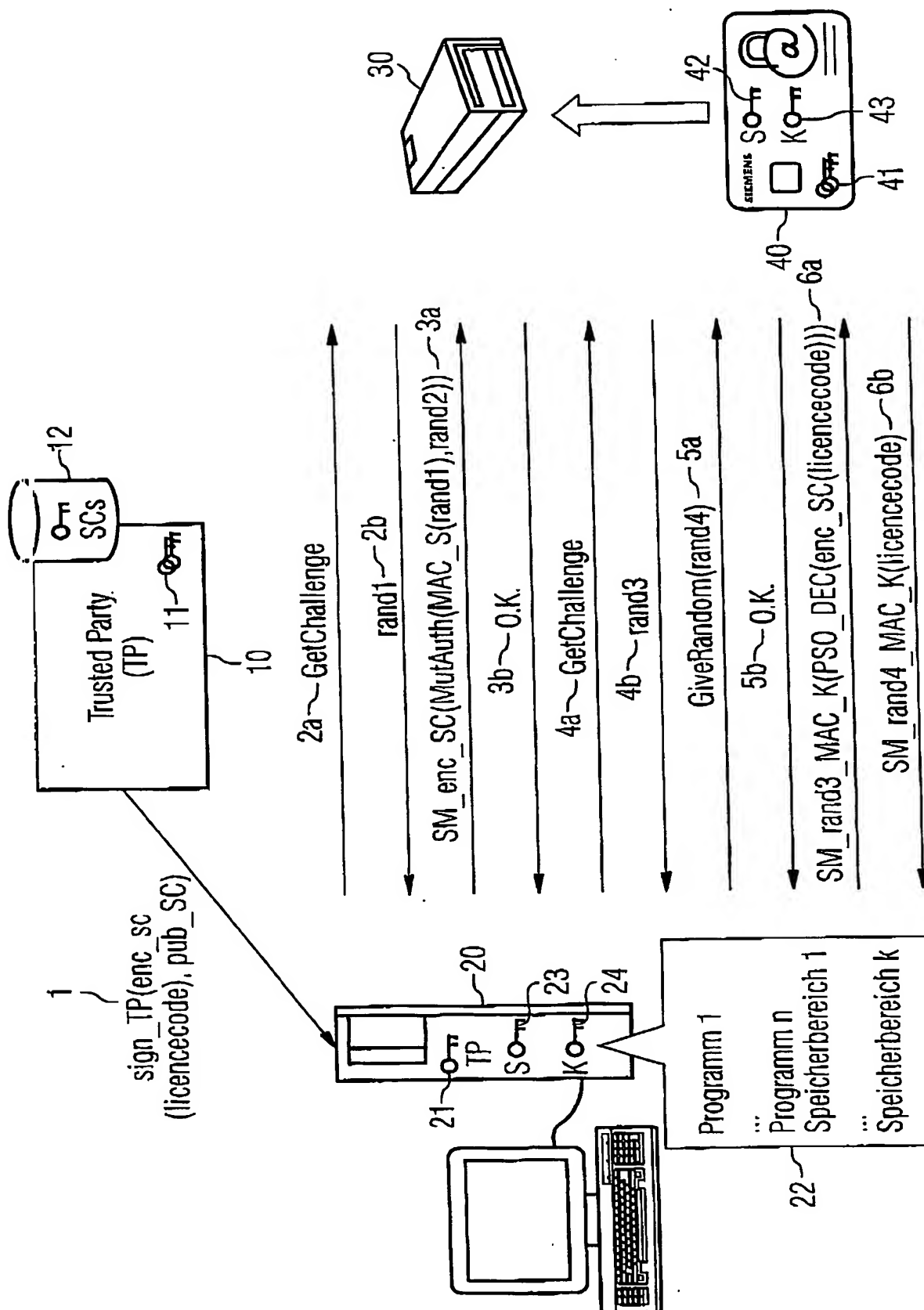
8. Verfahren nach Anspruch 7,
bei dem in der Recheneinrichtung eine vierte Zufallszahl erzeugt und diese an die Speicherkarte übermittelt wird, bei
25 dem durch die Speicherkarte für den entschlüsselten Lizenzcode ein Hash-Wert, der mittels des symmetrischen Schlüssels und der vierten Zufallszahl verschlüsselt wird, berechnet und verschlüsselt an die Recheneinrichtung übermittelt wird, und
bei dem der mittels des symmetrischen Schlüssels und der
30 vierten Zufallszahl verschlüsselte Hash-Wert in der Recheneinrichtung entschlüsselt und mit einem für den entschlüsselten Lizenzcode berechneten Hash-Wert auf Übereinstimmung überprüft wird.

35 9. Verfahren nach einem der Ansprüche 1 bis 8,
bei dem zur Einräumung des Zugriffs auf das computerbasierte Objekt der entschlüsselte Lizenzcode und ein Überprüfungspro-

zeßverlauf mit einer jeweiligen Soll-Vorgabe abgeglichen werden.

10. Steuerungsprogramm, das in einen Arbeitsspeicher einer
5 Recheneinrichtung ladbar ist und zumindest einen Codeabschnitt aufweist, bei dessen Ausführung
- eine Erzeugung eines symmetrischen Schlüssels aus einer von einer Speicherkarte mit einem Programmcodeprozessor generierten ersten Zufallszahl und aus einer durch die Re-
10 cheneinrichtung bereitgestellten zweiten Zufallszahl veranlaßt wird,
 - eine Übermittlung eines mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcodes und einer mit einem unter Verwendung des symmetrischen Schlüssels verschlüsselten Hash-Wert versehenen Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes an die Speicherkarte veranlaßt wird,
 - eine Entschlüsselung des verschlüsselten Hash-Werts durch
20 die Speicherkarte und eine Überprüfung auf Übereinstimmung mit einem für die Angabe der von der Speicherkarte auszuführenden Funktion berechneten Hash-Wert veranlaßt wird,
 - bei positivem Überprüfungsergebnis eine Ausführung der Funktion zur Entschlüsselung des Lizenzcodes durch die
25 Speicherkarte und eine Übermittlung eines entschlüsselten Lizenzcodes an die Recheneinrichtung veranlaßt werden,
 - der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt durch die Recheneinrichtung bereitgestellt wird,
- 30 wenn das Steuerungsprogramm in der Recheneinrichtung abläuft.

1/1



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052243

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 076 279 A (HEWLETT PACKARD CO) 14 February 2001 (2001-02-14) paragraphs '0001!', '0008!', '0012!', '0026!', '0027!', '0037!', '0043!', '0046!', '0056!', '0065!', '0069!', '0157!', '0160!', '0171!'-----	1-10
X	US 2003/161473 A1 (FRANSDONK ROBERT W) 28 August 2003 (2003-08-28) paragraphs '0017!', '0076!', '0086!', '0097!', '0299!; figure 16 ----- -/--	1-10

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

11 January 2005

Date of mailing of the international search report

19/01/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Kerschbaumer, J

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052243

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIER B: "AUTHENTICATION" APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, 1996, pages 52-65, 178, XP002908685 ISBN: 0-471-11709-9 pages 59-63	1-10
A	EP 0 803 789 A (EUROP COMPUTER IND RES) 29 October 1997 (1997-10-29) column 7, line 1 - line 44	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/052243

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1076279	A	14-02-2001	EP 1076279 A1	14-02-2001
			DE 60002893 D1	26-06-2003
			DE 60002893 T2	13-05-2004
			EP 1203278 A1	08-05-2002
			EP 1204910 A1	15-05-2002
			WO 0113198 A1	22-02-2001
			WO 0113199 A1	22-02-2001
			JP 2003507784 T	25-02-2003
			JP 2003507785 T	25-02-2003
<hr/>				
US 2003161473	A1	28-08-2003	AU 6985601 A	02-01-2002
			EP 1407360 A1	14-04-2004
			US 2003161476 A1	28-08-2003
			US 2003165241 A1	04-09-2003
			US 2003163684 A1	28-08-2003
			US 2003161335 A1	28-08-2003
			US 2003167392 A1	04-09-2003
			WO 0198903 A1	27-12-2001
<hr/>				
EP 0803789	A	29-10-1997	AU 716912 B2	09-03-2000
			AU 1912097 A	30-10-1997
			EP 0803789 A2	29-10-1997
			US 5935246 A	10-08-1999
<hr/>				

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/052243

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RESEARCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 076 279 A (HEWLETT PACKARD CO) 14. Februar 2001 (2001-02-14) Absätze '0001!', '0008!', '0012!', '0026!', '0027!', '0037!', '0043!', '0046!', '0056!', '0065!', '0069!', '0157!', '0160!', '0171!' -----	1-10
X	US 2003/161473 A1 (FRANSDONK ROBERT W) 28. August 2003 (2003-08-28) Absätze '0017!', '0076!', '0086!', '0097!', '0299!; Abbildung 16 ----- ----- -/-	1-10

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

11. Januar 2005

Absenddatum des Internationalen Recherchenberichts

19/01/2005

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Kerschbaumer, J

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/052243

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	SCHNEIER B: "AUTHENTICATION" APPLIED CRYPTOGRAPHY. PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, NEW YORK, JOHN WILEY & SONS, US, 1996, Seiten 52-65,178, XP002908685 ISBN: 0-471-11709-9 Seiten 59-63	1-10
A	EP 0 803 789 A (EUROP COMPUTER IND RES) 29. Oktober 1997 (1997-10-29) Spalte 7, Zeile 1 - Zeile 44	1-10

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/052243

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1076279 A	14-02-2001	EP 1076279 A1	14-02-2001
		DE 60002893 D1	26-06-2003
		DE 60002893 T2	13-05-2004
		EP 1203278 A1	08-05-2002
		EP 1204910 A1	15-05-2002
		WO 0113198 A1	22-02-2001
		WO 0113199 A1	22-02-2001
		JP 2003507784 T	25-02-2003
		JP 2003507785 T	25-02-2003
US 2003161473 A1	28-08-2003	AU 6985601 A	02-01-2002
		EP 1407360 A1	14-04-2004
		US 2003161476 A1	28-08-2003
		US 2003165241 A1	04-09-2003
		US 2003163684 A1	28-08-2003
		US 2003161335 A1	28-08-2003
		US 2003167392 A1	04-09-2003
		WO 0198903 A1	27-12-2001
EP 0803789 A	29-10-1997	AU 716912 B2	09-03-2000
		AU 1912097 A	30-10-1997
		EP 0803789 A2	29-10-1997
		US 5935246 A	10-08-1999